UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

ONLY CHOICE URGENT CARE & MED SPA and STEWART SCHARFMAN PHYSICAL THERAPY, PC, on behalf of themselves and all others similarly situated, Plaintiffs, v. UNITEDHEALTH GROUP INCORPORATED, UNITEDHEALTHCARE, INC., OPTUM, INC., and CHANGE HEALTHCARE INC., Defendants.	**Civil Action No.:** **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiffs Only Choice Urgent Care & Med Spa and Stewart Scharfman Physical Therapy, PC ("Plaintiffs"), individually and on behalf of all others similarly situated ("Class Members"), bring this class action against Defendants UnitedHealth Group Incorporated ("UnitedHealth"), UnitedHealthcare, Inc. ("UnitedHealthcare"), and Optum, Inc. ("Optum"), Change Healthcare Inc. ("Change") (collectively, "Defendants") for their failure to properly secure and safeguard their systems from foreseeable cyberattacks that impacted Plaintiffs' business operations and Plaintiffs' and Class Members' personally identifiable information ("PII") and financial account information stored within Defendants' information network. Plaintiffs make these allegations on personal information as to those allegations pertaining to themselves and their personal circumstances, and upon information and belief, based on the investigation of counsel and facts that are matters publicly known, on all other matters.

INTRODUCTION

1. This action arises from Defendants' provision of diverse services to healthcare providers and pharmacies. These services encompass clearinghouse functions, enabling providers to electronically submit claims to insurance companies, and facilitating electronic payments from insurers to providers.

2. Defendant Change, a division of UnitedHealth's Optum subsidiary, is a significant player in the realm of health technology. It offers crucial revenue and payment cycle management services that form the backbone of the U.S. healthcare system. These services establish vital connections among payers, providers, pharmacies, and patients. Change plays an indispensable role in nationwide healthcare delivery.

3. Change holds the distinction of being the largest commercial prescription processor in the nation. It acts as a digital intermediary, verifying a patients' insurance coverage for prescriptions, processing manufacturer-provided "coupons" and "co-pay" cards to assist patients in affording medications and treatments, including those who are uninsured or under-insured. Moreover, it manages prescriptions and billing for over 67,000 pharmacies across the U.S. healthcare network. The systems operated by Change handle a vast amount of data, including confidential patient health information and banking details for providers.

4. Change states it handles 15 billion healthcare transactions annually, encompassing various services that directly impact patient care, such as clinical decision support, eligibility verifications, and pharmacy operations. It interacts with one out of every three U.S. patient records, and its cloud-based network facilitates "14 billion clinical, financial, and operational transactions annually."

5. Defendants serve as the central hub of the nationwide health insurance claims processing network. In the course of their routine operations, Defendants gathered, digitized, aggregated, organized, and stored health insurance claims-related data belonging to Plaintiffs and Class members, including PII of Plaintiffs, Class members, and their patients. Given the breadth of Defendants' operations and the volume of sensitive information they manage, it is evident that they present an enticing target for cyberattacks.[1] "If you're going to go after stealing records, you want to go after the biggest pot of records you can get," said Fred Langston, the chief product officer for Critical Insight, a cybersecurity firm.[2]

6. On February 21, 2024, UnitedHealth, the nation's largest insurer, submitted a Form 8-K to the Securities and Exchange Commission revealing that Change's systems had been infiltrated by a "suspected nation-state associated cyber security threat actor."[3] "[T]he network interruption is [believed to be] specific to Change Healthcare systems, and all other systems across the Company are operational. During the disruption, certain networks and transactional services may not be accessible."[4]

7. Subsequent reports identified the cybercriminals who breached Change's system as the ransomware gang ALPHV/Blackcat ("Blackcat"). Blackcat not only claimed responsibility for the attack but also asserted it had infiltrated and extracted confidential information, including health information, for millions of patients (referred to as the "Data Breach").

8. According to reports, the attack took the form of a ransomware attack, during which Blackcat gained access to multiple terabytes of sensitive health data in exchange for a

[1] NY Times Reed Abelson Feb. 26, 2024 A Cyberattack on a UnitedHealth Unit Disrupts Prescription Drug Orders, https://www.nytimes.com/2024/02/26/health/cyberattackprescriptions-united-healthcare.html (last visited Mar. 28, 2024)
[2] *Id.*
[3] UnitedHealth Group Inc., SEC Filing Form 8-K Filing, filed February 21, 2024.
[44] *Id.*

substantial ransom payment. It appears that approximately $22 million was paid to secure the release of the data.

9. The Data Breach, targeting one of America's largest healthcare companies, was described by the American Hospital Association as "the most serious incident of its kind leveled against a U.S. health care organization."

10. The attack was entirely foreseeable and prevented. In fact, in a Joint Cybersecurity Advisory released on December 19, 2023, the Federal Bureau of Investigation ("FBI") and the Cybersecurity & Infrastructure Security Agency ("CISA") urged critical infrastructure organizations, such as Defendants, to implement the recommendations outlined in the advisory to mitigate the likelihood and impact of inevitable ransomware and data extortion attempts by groups like Blackcat. The FBI and CISA provided detailed technical information about the Blackcat criminal organization and its attack methods, and advised organizations to take immediate action, including to "prioritize remediation of known exploited vulnerabilities."[5]

11. Despite these urgent and critical warnings being made public, it is evident from the reported scope and severity of the attack that Defendants failed to undertake reasonably, timely, and adequate measures to defend against the foreseeable and devastating cyberattack, including remediation ("patching") the known vulnerabilities.

12. Defendants did not detect the breach until it was too late. The cyberattack was a ransomware attack that incapacitated Defendants' systems for weeks, disrupting the claims process and causing delays in the processing and payment of insurance claims.

13. Plaintiffs and Class members are healthcare providers or professionals who were injured as a result of the unauthorized disclosure of their PII, and the disruption to their access to

[5] *See* FBI and CISA Joint Cybersecurity Advisory (December 19, 2023), available at: jointcybersecurity-advisory-tlp-clear-stopransomware-alphv-blackcat-12-19-2023.pdf (aha.org).

Defendants' networks and transactional services, including the loss of access to Defendants' insurance claims clearinghouse and loss of income from insurance claims. Plaintiffs and Class members seek damages and injunctive relief for the injuries they sustained as a result of the Data Breach, which continues to negatively impact their businesses.

PARTIES

14. Plaintiff Only Choice Urgent Care & Med Spa is a Texas professional corporation with its principal place of business in Huffman, Texas. Only Choice provides affordable essential healthcare and alternative services to the emergency room for its patients.

15. Plaintiff Stewart Scharfman Physical Therapy, PC is a New York corporation with its principal place of business in Floral Park, New York. Scharfman provides physical therapy services to its patients.

16. Defendant UnitedHealth Group Inc. is a Delaware corporation with its principal place of business in Minnetonka, Minnesota.

17. Defendant UnitedHealthcare, Inc. is a Delaware corporation with its principal place of business in Minnetonka, Minnesota.

18. Defendant Optum, Inc. is a Delaware corporation with its principal place of business in Eden Prairie, Minnesota.

19. Defendant Change Healthcare, Inc. is a Delaware corporation with its principal place of business in Nashville, Tennessee.

JURISDICTION AND VENUE

20. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000 exclusive of interest and costs, there are more than 100 members in the

proposed class, and at least one member of the class, including Defendant, is a citizen of a state different from Defendant. This Court has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367 because all claims alleged herein form part of the same case or controversy.

21. This Court has jurisdiction over Defendants because its principal place of business is in this District, regularly conducts business in Minnesota, and the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

22. Venue is proper under 18 U.S.C § 1391(b)(1) & (2) because Defendant's principal place of business is in this District, and a substantial part of the acts and omissions that form the basis of this Class Action Complaint occurred in this District.

FACTUAL ALLEGATIONS

Change's Business

23. Change is a "health technology giant" that provides revenue and payment cycle management that connects payers, providers, and patients within the U.S. healthcare system.

24. Change is regarded as the nation's largest commercial prescription processor, working with thousands of insurance companies, doctors, pharmacists, and hospitals to help determine patient responsibility for payment. Change handles prescriptions and billing for more than 67,00 pharmacies across the U.S. healthcare system.

25. According to Change, one-third of all U.S. patient records are "touched by [its] clinical connectivity solutions."[6] It processes 15 billion healthcare transactions annually – including a range of services that directly affect patient care, such as clinical decision support,

[6] Zack Whittaker, *As the Change Healthcare Outage Drags On, Fears Grow That Patient Data Could Spill Online*, TechCrunch (Mar. 9, 2024), https://techcrunch.com/2024/03/09/changehealthcare-fears-data-breach-ransomware/; Change Healthcare, https://www.changehealthcare.com/ (last visited Mar. 28, 2024).

eligibility verifications and pharmacy operations, and its "cloud-based network supports 14 billion clinical, financial, and operations transactions annually."[7]

26. Change states on its website: "The Change Healthcare Platform provides industry-leading analytics, expansive data, and unparalleled connection and data transfer between providers, payers, and consumers to help improve workflows, increase administrative and financial efficiencies, and improve clinical decisions."[8]

27. Change further states on its website: "We champion innovation through our unified platform to enable a better coordinated, more efficient, and increasingly collaborative healthcare system—one that enables operational efficiencies, optimizes financial performance, and enhances the healthcare experience."

28. Change is integral to the functioning of the U.S. healthcare sector, acting as a digital intermediary that helps pharmacies verify patients' insurance coverage for prescriptions.

29. Since its acquisition by UnitedHealth in 2022, Change has operated as a "unit" of Optum. Optum's services are used to facilitate health care for 132 million individual consumers; nearly 130,000 physicians; 90% of U.S. hospitals; 67,000 U.S. pharmacies; and 80% of U.S. health plans across all fifty states and the District of Columbia.[9]

30. UnitedHealth is ubiquitous in the United States healthcare system. Its umbrella of businesses touches nearly every aspect of the healthcare industry, including health insurance services, technology, data analytics, healthcare delivery, healthcare payor partner services, and

[7] https://www.changehealthcare.com/platform (last visited Marc. 28, 2024).

[8] https://www.changehealthcare.com/about (last visited Mar. 28, 2024).

[9] *Investor Conference 2023: Overview & Highlights*, Optum, https://www.unitedhealthgroup.com/content/dam/UHG/PDF/investors/2023/ic23/UHG_IC23_Optum_Overview_Highlights.pdf (last visited Mar. 28, 2024).

more.[10] In 2023, UnitedHealth reported earnings of $371.6 billion[11], ranking fifth on that year's Fortune 500 list.[12]

31. In the course of facilitating insurance and other transaction related to Plaintiff's and Class Members's healthcare, Defendants all receive, create, and handle patient PII and PHI, including, inter alia, names, addresses, Social Security numbers, medical records, payment information, prescription information, claims and insurance information, and other personal records.

32. With respect to PII and PHI, Change states on its website that it uses "Leading-Edge Technology" to secure customer payment information and accounts. According to Change, it "leverage[s] the latest technology, public and private data sources to fortify our processes and ensure your information is protected."[13]

33. Due to the sensitivity of the PII and PHI that Defendants handle, and their integral position in the healthcare system, Defendants are aware of their critical responsibility to safeguard their information systems as an outage of their network could jeopardize the health of millions of Americas, disrupting their access to vital mediations, and could subject individuals nationwide devastating consequences due to the theft of their sensitive personal information.

34. Despite the existence of these duties, Defendants failed to implement reasonable data security measures to safeguard their information systems, resulting in widescale disruption

[10] *Annual Report (Form 10-K)*, UnitedHealth Group (Feb. 28, 2024), https://www.unitedhealthgroup.com/content/dam/UHG/PDF/investors/2023/UNH-Q4-2023Form-10-K.pdf.
[11] *UnitedHealth Group Q4 Earnings Report*, UnitedHealth Group (Jan. 12, 2024), https://www.unitedhealthgroup.com/content/dam/UHG/PDF/investors/2023/UNH-Q4-2023Release.pdf.
[12] *Fortune 500*, Fortune, https://fortune.com/ranking/fortune500/ (last visited Mar. 28, 2024).
[13] https://support.changehealthcare.com/fraud-prevention (last visited Mar. 28, 2024).

to the U.S. healthcare system, including patients' access to vital medication, and allowing nefarious third-party cybercriminals to compromise Plaintiff's and Class members' PII and PHI.

The Data Breach

35. Defendants provide numerous healthcare and insurance-related services. Defendants' wholly owned subsidiary, Change Healthcare, provides claims management for healthcare providers, like hospitals, pharmacies, and physicians and other healthcare providers.

36. On or about February 21, 2024, Change experienced a data breach event (i.e., the Data Breach) through which (on information and belief) Plaintiff's and Class Members' Private Information in possession of Change and/or Defendants was obtained by an unauthorized party. According to publicly available information, including statements by Defendants, Change's systems were accessed by cybercriminals.

37. According to publicly available information, the data breach event was a ransomware attack, wherein the cybercriminals accessed Change's systems and encrypted Change's (and, upon information and belief, multiple other entities') data to hold it hostage with the aim of securing a large ransom payment.

38. In a Form 8-K report filed with the Securities Exchange Commission on February 21, 2024, UnitedHealth stated:

> **Item 1.05. Material Cybersecurity Incidents.**
>
> On February 21, 2024, UnitedHealth Group (the "Company") identified a suspected nation state associated cyber security threat actor had gained access to some of the Change Healthcare information technology systems. Immediately upon detection of this outside threat, the Company proactively isolated the impacted systems from other connecting systems in the interest of protecting our partners and patients, to contain, assess and remediate the incident.

> The Company is working diligently to restore those systems and resume normal operations as soon as possible, but cannot estimate the duration or extent of the disruption at this time. The Company has retained leading security experts, is working with law enforcement and notified customers, clients and certain government agencies. At this time, the Company believes the network interruption is specific to Change Healthcare systems, and all other systems across the Company are operational.
>
> During the disruption, certain networks and transactional services may not be accessible. The Company is providing updates on the incident at https://status.changehealthcare.com/incidents/hqpjz25fn3n7. Please access that site for further information.
>
> As of the date of this report, the Company has not determined the incident is reasonably likely to materially impact the Company's financial condition or results of operations. [emphasis in original]

39. On or about February 28, 2024, notorious cybercrime group Blackcat claimed on its darknet site responsibility for the attack, claiming it stole from Change millions of sensitive records—over eight terabytes of data—including medical insurance and health data on thousands of healthcare providers, pharmacies, and insurance providers.

40. One day later, on February 29, 2024, UnitedHealth confirmed the ransomware attack on its subsidiary, stating: "Change Healthcare can confirm we are experiencing a cyber

security issue perpetrated by a cybercrime threat actor who has represented itself to us as ALPHV/Blackcat."[14]

41. Media sources indicate that, on March 1, 2024, Change paid to ALPHV Blackcat a ransom in response to the attack, in the amount of 350 bitcoins, or approximately $22 million.[15]

42. The Data Breach was carried out by a ransomware attack that has been known, forensically analyzed, documents, and remediated since at least April 19, 2022, when the Federal Bureau of Investigation published FLASH No. CU-000167-MW "BlackCat/ALPHV Ransomware Indicators of Compromise."

43. Like more cyberattack attempts, it starts by obtaining compromised user credentials to gain initial access to the system. *Id.* From there, the hackers employ techniques to disable security features and execute the ransomware, which encrypts files and data, locking out access to critical systems and information. The hackers then demand payment in cryptocurrency in exchange for providing the key to decrypt the files. Ransomware attack attempts are prevalent and are eminently foreseeable by Defendants, whose digitization, organization, compilation, and maintenance of highly valuable sensitive personal, health, and financial information make it a prime target for hackers.

44. Defendants failed to adequately protect their systems, failed to adequately prepare for known threats, and failed to reasonably prevent the breadth and scope of the Data Breach. The FBI alert details many "Recommended mitigations" to prevent and limit the threat of the Blackcat ransomware, and Defendants failed to follow these measures:

---

[14] Joseph Menn, *Hacking gang behind pharmacy chaos shuts down again. Will it matter?* (March 6, 2024) https://www.washingtonpost.com/technology/2024/03/06/ransomware-gang-alphv-shuts-down/ (last visited Mar. 28, 2024).
[15] *Id.*

a. Review domain controllers, servers, workstations, and active directories for new or unrecognized user accounts.

b. Regularly back up data, air gap, and password protect backup copies offline. Ensure copies of critical data are not accessible for modification or deletion from the system where the data resides.

c. Review Task Scheduler for unrecognized scheduled tasks. Additionally, manually review operating system defined or recognized scheduled tasks for unrecognized "actions" (for example: review the steps each scheduled task is expected to perform).

d. Review antivirus logs for indications they were unexpectedly turned off.

e. Implement network segmentation.

f. Require administrator credentials to install software.

g. Implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, secure location (e.g., hard drive, storage device, the cloud).

h. Install updates/patch operating systems, software, and firmware as soon as updates/patches are released.

i. Use multifactor authentication where possible.

j. Regularly change passwords to network systems and accounts, and avoid reusing passwords for different accounts.

k. Implement the shortest acceptable timeframe for password changes.

l. Disable unused remote access/Remote Desktop Protocol (RDP) ports and monitor remote access/RDP logs.

m. Audit user accounts with administrative privileges and configure access controls with least privilege in mind.

n. Install and regularly update antivirus and anti-malware software on all hosts.

45. Most recently in December 2023, the Joint Cybersecurity Advisory (CSA) published a report, warning that Blackcat targets the healthcare sector the most. The advisory provided significant details about methods of attack, including tactics, indicators of compromise, and screenshots of messages from the hackers.

46. The December advisory emphasized additional measures to protect against the attack:

a. Secure remote access tools by:

i. **Implementing application controls** to manage and control execution of software, including allowlisting remote access programs. Application controls should prevent installation and execution of portable versions of unauthorized remote access and other software. A properly configured application allow listing solution will block any unlisted application execution. Allowlisting is important because antivirus solutions may fail to detect the execution of malicious portable executables when the files use any combination of compression, encryption, or obfuscation.

ii. Applying recommendations in CISA's joint Guide to Securing Remote Access Software.

b. **Implementing FIDO/WebAuthn authentication or Public key Infrastructure (PKI)-based MFA** [CPG 2.H][HPH CPG – Multifactor Authentication]. These MFA implementations are resistant to phishing and not susceptible to push

bombing or SIM swap attacks, which are techniques known to be used by ALPHV Blackcat affiliates. See CISA's Fact Sheet Implementing Phishing-Resistant MFA for more information.

c. **Identify, detect, and investigate abnormal activity and potential traversal of the indicated ransomware with a networking monitoring tool.** To aid in detecting ransomware, implement a tool that logs and reports all network traffic [CPG 5.1][HPH CPG – Detect and Respond to Relevant Threats and Tactics, Techniques and Procedures], including lateral movement activity on a network. Endpoint detection and response (EDR) tools are useful for detecting lateral connections as they have insight into common and uncommon network connections for each host.

d. **Implement user training on social engineering and phishing attacks** [CPG 2.I][HPH CPG – Basic Cybersecurity Training]. Regularly educate users on identifying suspicious emails and links, not interacting with those suspicious items, and the importance of reporting instances of opening suspicious emails, links, attachments, or other potential lures.

e. **Implement internal mail and messaging monitoring.** Monitoring internal mail and messaging traffic to identify suspicious activity is essential as users may be phished from outside the targeted network or without the knowledge of the organizational security team. Establish a baseline of normal network traffic and scrutinize any deviations.

f. **Implement free security tools** to prevent cyber threat actors from redirecting users to malicious websites to steal their credentials. For more information see, CISA's Free Cybersecurity Services and Tools webpage.

g. **Install and maintain antivirus software.** Antivirus software recognizes malware and protects your computer against it. Installing antivirus software from a reputable vendor is an important step in preventing and detecting infections. Always visit vendor sites directly rather than clicking on advertisements or email links. Because attackers are continually creating new viruses and other forms of malicious code, it is important to keep your antivirus software up to date.

47. Defendants failed to take these steps, which they had a duty of care and legal obligations to undertake, and caused, facilitated, and failed to detect, limit, and prevent the Data Breach.

48. As a result of the Data Breach, Plaintiffs and Class members had their PII accessed and stolen by criminals and were unable to have their claims processed and paid for an extended period of time. As a result of the disruption, Plaintiffs and Class members suffered injuries due to the lack of cash flow, loss of revenue, loss of time, and out-of-pocket expenses to mitigate the damages and learn about the Data Breach and institute work arounds to keep their businesses afloat over the extended period of time that Defendants were down.

The Data Breach Caused an Unprecedented Disruption in the Provision of Healthcare Throughout the Nation

49. Given the centrality of the Defendants in the healthcare field, the impact of the Data Breach has rippled to virtually every segment of the healthcare industry. But, as is too often the case, the effect was felt most acutely on small businesses. The American Medical Association ("AMA") described the Data Breach as an "unprecedented disruption to medical

practices and access to care." "Physicians are experiencing financial struggles that threaten the viability of many medical practices. Many physician practices operate on thin margins, and the AMA is especially concerned about the impact on small and rural practices, as well as those that care for the underserved."[16]

50. A spokesman for UnitedHealth estimated that more than 63,000 pharmacies nationwide have been affected by the attack.[17]

51. In addition to the impact on prescription medication, healthcare providers throughout the U.S. were locked out of processing payments and, in turn, were "struggling to get paid" following the ransomware outage, resulting in overdue payments, interest accumulation, and other financial harm.[18]

52. Plaintiffs learned about the Data Breach after the systems went down and heard the story from the news shortly after the Data Breach was publicly announced.

53. Plaintiffs' practice employed a software program called TherapyNotes, which among other things, Plaintiffs used to submit insurance claims for payment of services rendered to patients. Through TherapyNotes, Plaintiffs used Defendants' claims clearinghouse to facilitate the submission and payment of insurance claims.

54. According to TherapyNotes, "Therapy notes' services that were affected included Electronic claim submission (including EDI-to-paper claims), ERAs, and real-time eligibility

[16] March 5, 2024 Press Release, https://www.webwire.com/ViewPressRel.asp?aId=318864.
[17] *WA pharmacies, health systems reel from UnitedHealthcare cyberattack* (February 29, 2024), available at: https://www.seattletimes.com/seattle-news/health/wa-pharmacies-health-systemsreel-unitedhealthcare-cyberattack/ (last visited Mar. 28, 2024).
[18] According to the proprietor of a Michigan laboratory, over a week after the cyberattack, the lab remained "100 percent down when it comes to billing right now," while six small providers reported to Reuters that "they were unable to process claims and were racking up thousands of dollars in overdue payments." *Healthcare providers hit by frozen payments in ransomware outage*, Reuters (February 29, 2024), available at: https://www.msn.com/enus/money/companies/healthcare-providers-hit-by-frozen-payments-in-ransomware-outage/ (last visited Mar. 28, 2024).

(RTE) checks are all down during this outage." ERA means electronic remittance advice, which is an explanation from a health plan to a provider about a claim payment.

55. Plaintiffs suffered substantial hardship as a result of the Data Breach. Without payments from insurance companies, Plaintiffs lost the vast majority of their income stream. Plaintiffs had difficulty meeting operation expenses. Many Plaintiffs and Class members were forced with the undesirable need to withdraw funds, ask for a line of credit at their local banks, or put a second mortgage on their homes to meet payroll and other business expenses. In addition, Plaintiffs spent considerable time and effort, were diverted from income-generating work, by having to react to the outage, mitigate their damages, and find workarounds, monitor accounts and personal information, and/or eventually switch to manually submitting claims through other competing products/systems such as OfficeAlly.

56. Meanwhile, Defendants (who are also insurance companies) and other insurance companies like it, continued to collect insurance premiums, and enriched themselves during the period of time they were being paid for coverage they did not provide as a result of the Data Breach.

57. Because OfficeAlly or other products have different requirements, Plaintiffs will have to get accustomed to a whole new system. For example, Payer IDs may be different so claims may get delayed or lost as a result. Plaintiffs and Class members have had to and will have to diligently monitor the manual submission of claims and the processing to ensure that claims are processed timely and accurately.

58. The U.S. Department of Health and Human Services issued a press release stating "HHS recognizes the impact this attack has had on health care operations across the country. HHS' first priority is to help coordinate efforts to avoid disruptions to care throughout the health

care system."[19] The release provides guidance to Medicare providers to contact their Medicare Administrative Contractor to request a new electronic data interchange enrollment to switch clearinghouse, recommends relaxing or removing preauthorization and utilization requirements, and suggests that insurance companies "advance funding to providers," on behalf of Medicaid and CHIP-managed care enrollees.

59. Plaintiffs and Class members have suffered and will continue to suffer injuries as a result of the theft of their PII, their loss of revenues, loss of services, and implementing workarounds to just to get their businesses working as usual.

60. Defendants' response has been insufficient and self-interested. Defendants failed to provide direct notice to impacted persons. Instead, many victims like Plaintiffs had to learn about the Data Breach by reading about it in the news.

61. An inconspicuous banner at the top of changehealthcare.com's web page links to "Information on the Change Healthcare Cyber Response." As of March 7, 2024, it was still working on mitigating the impact of the Data Breach, promising that "electronic payment functionality will be available for connection beginning March 15." And, "We expect to begin testing and reestablish connectivity to our claims network and software on March 18, restoring service through the week."

62. Optum, part of the Change Healthcare ecosystem, offered impacted practices and hospitals a so-called Temporary Funding Assistance Program "to help bridge the gap in short-term cash flow needs for providers." However, to enroll, one must agree to Defendants' Privacy Policy (i.e., permit them to collect personal sensitive information and computer activity information), provide Defendants with additional personal and financial information, and agree

[19] https://www.hhs.gov/about/news/2024/03/05/hhs-statement-regarding-the-cyberattack-onchange-healthcare.html. (last visited Mar. 29, 2024)

to their adhesive terms of service (which seek to unconscionably impose one-sided terms on practices hard-strapped for operating expenses as a direct result of Defendants' unlawful conduct).

63. Independent groups are advising caution against believing Defendants' assurances that other systems and offerings are safe and secure. The AMA advises "with consideration of the written attestation from [Defendants] that the Optum network is safe, organizations should evaluate their risk of using Optum, UnitedHealthcare and UHG systems."

64. TherapyNotes advises its users to "please hold on registering for [Optum's temporary loan program]."[20]

65. The Wall Street Journal reports that those who do seek a loan do not [but]receive "anywhere close to what they need."[21] Examples cited in the article include someone who sought $30,000 but was offered $190, after spending all that time submitting an application.[22]

Defendants Are Liable to Plaintiffs and Class Members

66. Defendants are large, sophisticated organizations with the resources to deploy robust cybersecurity protocols. They knew or should have known, that the development and use of such protocols were necessary to fulfill their statutory and common law duties to Plaintiffs and Class members. Therefore, their failure to do so is intentional, willful, reckless and/or grossly negligent.

67. Defendants disregarded the rights of Plaintiffs and Class members by, *inter alia*, (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that their network servers were protected against unauthorized intrusions; (ii)

[20] https://blog.therapynotes.com/change-healthcare-incident-faq (last visited Mar. 28, 2024).
[21] https://www.wsj.com/articles/calls-mount-for-government-help-as-change-healthcare-hackfreezes-medical-payments-9545d2e3 (last visited Mar. 28, 2024).
[22] *Id.*

failing to disclose that they did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiffs' and Class members' PII; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (v) failing to provide Plaintiffs and Class members prompt and accurate notice of the Data Breach.

68. As a result of Defendants' ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of the cyberattack, the risk of identity theft, business interruption, disruption to continuity of care to the Plaintiffs and Class members has materialized and is present and continuing, and Plaintiffs and Class members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threats presented by the Data Breach; (c) the loss of benefit of the bargain (price premium damages); (d) diminution of value of the services they were entitled to enjoy; and (e) the continued risk and disruptions to their business operations going forward while they implement changes and workarounds.

69. Plaintiffs and Class members have spent and will spend additional time in the future, on a variety of prudent actions to remedy the harms they have or may experience as a result of the Data Breach, such as researching and verifying the legitimacy of the Data Breach.

CLASS ALLEGATIONS

70. Plaintiffs bring this action pursuant to the provisions of Federal Rule of Civil Procedure 23 on behalf of themselves and the following Class:

> ***Nationwide Class:*** All healthcare providers in the United States who used or attempted to use Defendants' networks and transactional services from the time of the Data Breach, reported on February 21, 2024, to the present.

71. Excluded from the Class are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendants have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as immediate family members.

72. Plaintiffs reserve the right to amend the above definitions or to propose subclasses in subsequent pleadings and motions for class certification.

73. This action has been brought and may properly be maintained as a class action under Federal Rule of Civil Procedure Rule 23 because there is a well-defined community of interest in the litigation, and membership in the proposed classes is easily ascertainable.

74. **Numerosity (Federal Rule of Civil Procedure 23(a)(1))**: Joinder of all class members is impractical because Defendants process 15 billion claims annually and class members are geographically dispersed.

75. **Commonality (Federal Rule of Civil Procedure 23(a)(2) and (b)(3))**: Plaintiffs and the Class members share a community of interests in that there are numerous common questions and issues of fact and law which predominate over any questions and issues solely affecting individual members, including, but not necessarily limited to:

a. Whether Defendants had a legal duty to Plaintiffs and Class members to exercise due care in collecting, storing, using, and/or safeguarding the sensitive information targeted in the Data Breach;

b. Whether Defendants knew or should have known of the susceptibility of their data security systems to the Data Breach;

c. Whether the Defendants' security procedures and practices to protect their systems were reasonable in light of the measures publicly available and recommended by data security experts;

d. Whether Defendants' failure to implement adequate data security measures facilitated, caused, and exacerbated the Data Breach;

e. Whether Defendants failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

f. Whether Defendants adequately, promptly, and accurately informed Plaintiffs and Class members of the Data Breach;

g. Whether Defendants have or will adequately address and fix the vulnerabilities which permitted the Data Breach to occur;

h. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to prevent the Data Breach;

i. Whether Plaintiffs and Class members are entitled to actual and/or statutory damages and/or whether injunctive, corrective and/or declaratory relief and/or accounting is/are appropriate as a result of Defendants' wrongful conduct; and

j. Whether Plaintiffs and Class members are entitled to restitution as a result of Defendants' wrongful conduct.

76. **Typicality (Federal Rule of Civil Procedure 23(a)(3))**: Plaintiffs' claims are typical of Class members' claims. Plaintiffs and Class members were uniformly impacted by the

Data Breach, sustained damages arising out of and caused by Defendants' common course of conduct in violation of law.

77. **Adequacy of Representation (Federal Rule of Civil Procedure 23(a)(4))**: Plaintiffs are adequate Class representatives. Plaintiffs have the same interest in the litigation as the Class members, are committed to the prosecution and just resolution of this case, and have retained competent counsel who are experienced in conducting litigation of this nature.

78. Plaintiffs are not subject to any individual defenses unique from those applicable to other Class members.

79. **Superiority of Class Action (Federal Rule of Civil Procedure 23(b)(3))**: Since the damages suffered by individual Class members, while not inconsequential, may be relatively small, the expense and burden of individual litigation by each member make or may make it impractical for members of the Class to seek redress individually for the wrongful conduct alleged herein. Should separate actions be brought or be required to be brought by each individual member of the Class, the resulting multiplicity of lawsuits would cause undue hardship and expense for the Court and the litigants.

80. The prosecution of separate actions would also create a risk of inconsistent rulings, which might be dispositive of the interests of the Class members who are not parties to the adjudications and/or may substantially impede their ability to protect their interests adequately.

81. This class action is also appropriate for certification because the Defendants have acted or refused to act on grounds generally applicable to Class members, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class members and making final injunctive relief appropriate with respect to the Class in its entirety.

82. Defendants' policies and practices challenged herein apply to and affect Class members uniformly and Plaintiff's challenge of these policies and practices hinges on Defendants' conduct with respect to the Class in its entirety, not on facts or law applicable only to Plaintiffs.

83. Unless a class-wide injunction is issued, Defendants may continue failing to properly secure their systems, and Defendants may continue to act unlawfully as set forth in this Complaint.

84. Further, Defendants have acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

CAUSES OF ACTION

COUNT ONE

Negligence

(On Behalf of Plaintiffs and the Nationwide Class)

85. Plaintiffs re-allege paragraphs 1–84 as if fully set forth herein.

86. At all times herein relevant, Defendants owed Plaintiffs and Class members a duty of care to act with reasonable care to secure and safeguard their PII and to use commercially reasonable methods to do so. Defendants took on this obligation upon themselves by agreeing to be in the business of a claims clearinghouse and payment processor and digitizing, aggregating, processing, and storing Plaintiffs' and Class members' healthcare-related data in their computer networks.

87. Among these duties, Defendants were expected:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Plaintiffs' and Class members' healthcare-related data;

b. to protect Plaintiffs' and Class members' healthcare-related data using reasonable and adequate security procedures and systems that were/are compliant with industry-standard practices;

c. to implement processes to detect the Data Breach quickly and to timely act on warnings about data breaches; and

d. to promptly notify Plaintiffs and Class members of any data breach, security incident, or intrusion that affected or may have affected their data and business operations.

88. Defendants knew that Plaintiffs' and Class members' healthcare-related data was private and confidential and should be protected as private and confidential and, thus, Defendants owed a duty of care not to subject Plaintiffs and Class members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

89. Defendants knew or should have known, of the risks inherent in collecting and storing Plaintiffs' and Class members' healthcare-related data, the vulnerabilities of their data security systems, and the importance of adequate security. As a result of Defendants' knowledge about their ability to repel hackers that Plaintiffs and Class members could not have known, and Defendants' public representations regarding its data security and privacy safeguards to the contrary, Defendants had a duty of care to disclose material facts of their susceptibility of attack, insufficient data security, and highly vulnerable systems critical to Plaintiffs' and Class members' practices.

90. Defendants knew about numerous, well-publicized data breaches.

91. Defendants knew and should have known that their data systems and networks did not adequately safeguard Plaintiffs' and Class members' healthcare-related data.

92. Only Defendants were in the position to ensure that their systems and protocols were sufficient to protect Plaintiffs' and Class members' healthcare-related data.

93. Defendants breached their duties to Plaintiffs and Class members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class members' healthcare-related data.

94. Because Defendants knew that a breach of their systems could damage millions of individuals, including Plaintiffs and Class members, Defendants had a duty to adequately protect their data systems and the data contained therein.

95. Plaintiffs' and Class members' willingness to entrust Defendants with their healthcare-related data was predicated on the understanding that Defendants would take adequate security precautions.

96. Moreover, only Defendants had the ability to protect their systems from attack. Thus, Defendants had a special relationship with Plaintiffs and Class members.

97. Defendants also had independent duties under state and federal laws that required Defendants to reasonably safeguard Plaintiffs; and Class members' Plaintiffs' and Class members' healthcare-related data and promptly notify them about the Data Breach. These independent duties are untethered to any contract between Defendants, Plaintiffs, and/or the remaining Class members.

98. Defendants' willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

99. As a proximate and foreseeable result of Defendants' grossly negligent conduct, Plaintiffs and Class members have suffered damages and are at imminent risk of additional harms and damages.

100. To date, Defendants have not provided sufficient information to Plaintiffs and Class members regarding the extent of the unauthorized access and continue to breach their disclosure obligations and clearinghouse services obligations to Plaintiffs and Class members.

101. Further, through Defendants' failure to provide clear notification of the Data Breach, Defendants prevented Plaintiffs and Class members from taking meaningful, proactive steps to mitigate the effects of the Data Breach.

102. The damages Plaintiffs and Class members have suffered (as alleged above) and will suffer were and are the direct and proximate result of Defendants' grossly negligent conduct.

103. As a direct and proximate result of Defendants' negligence and negligence per se, Plaintiffs and Class members have suffered and will suffer injury.

104. As a direct and proximate result of Defendants' negligent actions and negligent omissions, Plaintiffs and Class members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, actual damages, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT TWO
Negligence *Per Se*
(On Behalf of Plaintiffs and the Nationwide Class)

105. Plaintiffs re-allege paragraphs 1–104 if fully set forth herein.

106. Defendants violated HIPAA regulations, including by:

a. Failing to ensure the confidentiality and integrity of electronic PHI that Defendants create, receive, maintain, and transmit, in violation of 45 C.F.R. section 164.306(a)(1);

b. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights, in violation of 45 C.F.R. section 164.312(a)(1);

c. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. section 164.308(a)(1);

d. Failing to identify and respond to suspected or known security incidents and mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 C.F.R. section 164.308(a)(6)(ii);

e. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI, in violation of 45 C.F.R. section 164.306(a)(2);

f. Failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 C.F.R. section 164.306(a)(3);

g. Failing to ensure compliance with HIPAA security standard rules by its workforce, in violation of 45 C.F.R. section 164.306(a)(4);

h. Impermissibly and improperly using and disclosing PHI that is and remains accessible to unauthorized persons, in violation of 45 C.F.R. section 164.502, *et seq.*;

i. Failing to effectively train all members of its workforce (including independent contractors) on the policies and procedures with respect to PHI as necessary and

appropriate for the members of its workforce to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. sections 164.530(b) and 164.308(a)(5); and,

j. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI in compliance with 45 C.F.R. section 164.530(c).

107. "Section 5 of the FTC Act [15 U.S.C. § 45] is a statute that creates enforceable duties, and this duty is ascertainable as it relates to data breach cases based on the text of the statute and a body of precedent interpreting the statute and applying it to the data breach context." In re Capital One Consumer Data Sec. Breach Litig., 488 F. Supp. 3d 374, 407 (E.D. Va. 2020). "For example, in F.T.C. v. Wyndham Worldwide Corp., 799 F.3d 236, 240 (3d Cir. 2015), the United States Court of Appeals for the Third Circuit affirmed the FTC's enforcement of Section 5 of the FTC Act in data breach cases." Capital One, 488 F. Supp. 3d at 407.

108. Plaintiffs' and Class members' healthcare-related data was and is nonpublic personal information and customer information.

109. Plaintiffs and Class members are in the group of persons that HIPAA and the FTC Act were enacted and implemented to protect, and the harms they suffered in the Data Breach as a result of Defendants' violations of HIPAA and the FTC Act were the types of harm the statutes and regulations are designed to prevent.

110. As a direct and proximate result of Defendants' numerous negligent acts and omissions, Plaintiffs and Class members are at a substantial, impending, and imminent risk of identity theft, and they have been forced to take mitigation steps, thereby incurring costs, to ensure their personal and financial safety.

111. As a direct and proximate result of the conduct of Defendants that violated HIPAA and the FTC Act, Plaintiffs and Class members have suffered actual and concrete injuries and will suffer additional injuries in the future, including economic and non-economic damages in the following forms: (a) invasion of privacy; (b) financial costs incurred mitigating the impact of the Data Breach; (c) loss of time and loss of productivity; (d) loss of use of services; and (e) unreasonable delay of payments for services rendered.

112. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class members are entitled to recover actual and punitive damages.

COUNT THREE
Breach of Implied Contract
(On Behalf of Plaintiffs and the Nationwide Class)

113. Plaintiffs re-allege paragraphs 1–84 as if fully set forth herein.

114. Defendants offered to provide goods and services to Plaintiffs and Class members in exchange for payment.

115. Defendants required Plaintiffs and Class members to provide their PII and claims information to receive these services.

116. In turn, Defendants agreed that they would not disclose the information and take reasonable steps to prevent a Data Breach. According to Defendants' privacy policy, Defendants "implement and maintain organizational, technical, and administrative security measures designed to safeguard the data [they] process against unauthorized access, destruction, loss, alteration, or misuse."

117. Implicit in the parties' agreement was that Defendants would take reasonable measures to prevent foreseeable data breaches, would take expedient measures to limit the effects of the Data Breach, and would provide Plaintiffs and Class members with prompt and adequate notice of all unauthorized access.

118. Plaintiffs and Class members would not have entrusted their information to Defendants without such an agreement.

119. Defendants materially breached the contracts by failing to safeguard such information, failing to limit the Data Breach, and failing to provide prompt and accurate notice of the Data Breach.

120. As a direct result of the Data Breach, Plaintiffs and Class members have suffered actual and concrete injuries and will suffer addition injuries into the future, including economic and non-economic damages in the following forms: (a) invasion of privacy; (b) financial costs incurred mitigating the impact of the Data Breach; (c) loss of time and loss of productivity; (d) loss of use of services; and (e) unreasonable delay of payments for services rendered.

COUNT FOUR
Bailment
(On Behalf of Plaintiffs and the Nationwide Class)

121. Plaintiffs re-allege paragraphs 1–84 as if fully set forth herein.

122. Plaintiffs' and Class members' information and records were provided to Defendants.

123. In delivering their information and records to Defendants, Plaintiffs and Class members intended and understood that they would be adequately safeguarded and protected.

124. Defendants accepted Plaintiffs' and Class members' information and records. By accepting, Defendants understood that Plaintiffs' and Class members' expectations regarding reasonable and adequate data security.

125. Accordingly, a bailment was established for the mutual benefit of the parties, and Defendants owed a duty to exercise reasonable care, diligence, and prudence in handling the information and records.

126. Defendants breached their duties of care by failing to take appropriate measures to safeguard and protect Plaintiffs' and Class members' information, resulting in the Data Breach.

127. As a direct result of the Data Breach, Plaintiffs and Class members have suffered actual and concrete injuries and will suffer addition injuries into the future, including economic and non-economic damages in the following forms: (a) invasion of privacy; (b) financial costs incurred mitigating the impact of the Data Breach; (c) loss of time and loss of productivity; (d) loss of use of services; and (e) unreasonable delay of payments for services rendered.

COUNT FIVE
Unjust Enrichment
(On Behalf of Plaintiffs and the Nationwide Class)

128. Plaintiffs re-alleges paragraphs 1–84 if fully set forth herein.

129. Defendants benefited from receiving Plaintiffs' and Class members' PII and records by its ability to retain and use that information for their own benefit.

130. Defendants also understood and appreciated that Plaintiffs' and Class members' information was private and confidential, and its value depended upon Defendants maintaining the privacy and confidentiality of that information.

131. Plaintiffs and Class members conferred a benefit upon Defendants by paying for its services, and in connection therewith, by providing their information to Defendants with the understanding that Defendants would implement and maintain reasonable data privacy and security practices and procedures. Plaintiffs and Class members should have received adequate protection and data security.

132. Defendants knew that Plaintiffs and Class members conferred a benefit which Defendants accepted. Defendants profited from these transactions and appreciated the benefits.

133. Defendants failed to provide reasonable security, safeguards, and protections to the information of Plaintiffs and Class members.

134. Defendants should not be permitted to retain money rightfully belonging to Plaintiffs and Class members, because Defendants failed to implement appropriate data security measures and caused the Data Breach.

135. Defendants accepted and wrongfully retained these benefits to the detriment of Plaintiffs and Class members.

136. Defendants' enrichment at the expense of Plaintiffs and Class members is and was unjust.

137. As a result of Defendants' wrongful conduct, as alleged above, Plaintiffs and Class members seek restitution of their money paid to Defendants, and disgorgement of all profits and benefits, imposition of a constructive trust, and other compensation obtained by Defendants, plus attorneys' fees, costs, and interest thereon.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all others similarly situated, respectfully requests that the Court enter judgment in their favor and for the following specific relief against Defendants as follows:

a. That the Court declare, adjudge, and decree that this action is a proper class action and certify the proposed class and/or any other appropriate subclasses under Fed. R. Civ. P.23 (b)(1), (b)(2), and/or (b)(3), including the appointment of Plaintiffs' counsel as Class Counsel;

b. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

c. That the Court enjoin Defendants, ordering them to cease from unlawful activities;

d. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiffs and Class members;

e. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class members.

f. For prejudgment interest on all amounts awarded, at the prevailing legal rate;

g. For an award of attorney's fees, costs, and litigation expenses, as allowed by law; and

h. For all other Orders, findings, and determinations identified and sought in this Complaint.

JURY TRIAL DEMANDED

Plaintiffs, on behalf of themselves and all others similarly situated, hereby demands a trial by jury of all issues in this complaint so triable.

Dated: April 10, 2024

Respectfully submitted,

By: */s/ Jacob R. Rusch*

Jacob R. Rusch (SBN 0391892)
Timothy Becker (SBN 025663)
Zackary Kaylor (SBN 0400854)
JOHNSON//BECKER, PLLC
444 Cedar Street, Suite 1800
St. Paul, MN 55101
Telephone: (612)436-1800
Facsimile: (612)436-1801
jrusch@johnsonbecker.com
tbecker@johnsonbecker.com
zkaylor@johnsonbecker.com

William M. Audet (CA SBN 117456)
Ling Y. Kuang (CA SBN 296873)
AUDET & PARTNERS, LLP

711 Van Ness Avenue, Suite 500
San Francisco, CA 94102-3275
Telephone:(415) 568-2555
Facsimile: (415) 568-2556
waudet@audetlaw.com
lkuang@audetlaw.com